Secure Storage - Application to Electronic Medical Chart

Kazuya Miyazaki
Hideyuki Ashihara

Summary

There has been rapid progress in computerization of important documents according to the trend of business computerization in corporations, government and other public office. It is expected that in the near future, some of the computerized documents must be preserved for more than decades.

Computerized data is generally different from paper-based documents or documents recorded on microfilms in that it is vulnerable to threats of alteration or leakage. However, we think it is possible to position electronic documents as legally valid and effective documents by countering such threats and by guaranteeing originality of the documents, and as a result, to truly move from paper-based system.

Secure storage is a technique utilizing the information security technology based on PKI (Public Key Infrastructures), which guarantees originality of electronic documents for long periods of time. It has such features as easiness in verifying originality of documents due to employment of a standard framework, and capability to keep originality of documents for long periods of time due to possession of a technique for extending a validity period.

Computerization has been in progress also in the medical field, and guidelines for storing medical records electronically have also been provided. This time, secure storage is applied to the electronic medical chart system becoming popular among the medical field, and study is made on its validity.

It is assumed the secure storage will be of benefit to introduce information technologies and to move from paper-based system not only in the medical field, but in many other fields.

Application of the secure storage to the electronic medical chart system

Medical chart data generated at in-hospital clients of local central hospitals, or medical chart data generated at electronic medical chart clients of collaborative medical facilities and collaborative nursing-care facilities is each transmitted via in-hospital medical chart server or electronic medical chart service provider, to the secure storage whereby original of the electronic medical charts are stored. The secure storage issues and manages electronic certificates to guarantee authenticity of the electronic medical charts, further collects secure timestamps and verification information of authentication documents to guarantee authenticity of the electronic medical charts for long periods of time, and performs extension of digital signatures.

1. Preface

According to the trend of business computerization in corporations, government and other public offices, there has been rapid progress in computerization of important documents, such as contract related documents, administrative documents, and electronic medical charts. It is not difficult to imagine that in the near future, we are obliged to preserve some documents to be computerized for five, ten, thirty years or longer term.

Computerized data is generally different from paper-based documents or documents recorded on microfilms in that it is vulnerable to threats in terms of security, like computerized data can be easily altered or switched etc. without leaving traces, or computerized data is subject to thefts, leakage or eavesdropping in large numbers and in secrecy. By countering such threats and by guaranteeing originality of the documents, we think it is possible to position electronic documents as legally valid and effective documents, and as a result, to truly move from paper-based system. As an effective technology for guaranteeing originality, there exists digital signature. According to Electronic Signature Law ("Law Concerning Electronic Signatures and Certification Services") enforced from April 1, 2001, the effectiveness of the digital signature is proved legally. However, the digital signature has several problems as well as its effect, therefore, it is not possible to guarantee originality of electronic documents for long periods of time just by appending digital signature to the electronic document.

The secure storage technique developed this time is a technique using the information security technology based on PKI, like digital signature, and whereby it is possible to guarantee originality of electronic documents for long periods of time.

In this article, it is shown brief description of secure storage, and application of the secure storage to electronic medical chart system as an example.

1. Necessity of storing electronic documents for long periods of time

It is required to preserve originals of some documents, such as various types of contracts, administrative documents, and electronic medical charts, for long periods of time according to legal or commercial practice. While computerization has been in progress, fact is that paper-based media and microfiches have been used for preserving documents for long periods of time to meet such requirements, since electronic documents have vulnerability as shown in the previous chapter.

To ensure originality of electronic documents, a scheme is needed to guarantee when, and by whom the electronic documents were drafted (or is admitted), and that the documents were not altered (these features are in sum referred to as authenticity of electronic documents). Digital signature in PKI is regarded as the most promising method to ensure authenticity of electronic documents, and legal support for digital signature is provided by Electronic Signature Law enforced from last year.

However, only usage of digital signatures can no more than guarantee "who draft an electronic document and that it is not altered", and cannot guarantee "when" the

document was drafted. Further, validity of digital signatures has temporal restriction: validity of digital signatures will be lost by expiration of validity period or revocation of a public-key certification, or putting keys and algorithms to be used for digital signatures under threat. Therefore, some kind of new scheme is needed to ensure authenticity of electronic documents for long periods of time using digital signatures.

3. Secure Storage

Secure storage is a technique to preserve electronic documents for long periods of time while ensuring authenticity. The general outline is shown below.

3.1 Guarantee of authenticity of electronic documents by electronic certificate

In the secure storage, registration, search, reference, and deletion etc. are performed according to requests by clients. In such a case, the secure storage issues and manages electronic certifications to guarantees the following contents (Fig. 1).

- The creator or the registration requesting party of a document
- The lodged document is not altered
- The fact and the day and time of access, such as registration, search, reference and deletion etc. to the documents

The electronic certification consists of information including a hash of the subject document, access information, a secure time stamp described in section 3 of chapter 3, and a corresponding digital signature for the information. Meanwhile, it is possible to maintain validity of the electronic documents for long periods of time thanks to the technique for retaining the legitimacy of digital signatures for long periods of time as described in section 2 of chapter 3. In comparison to the conventionally proposed technique to ensure originality of documents by using tamper-proof hardware, whereby it has been difficult to verify the legitimacy of originality objectively, the technique now developed is implemented by software according to PKI, and therefore a third party can verify the legitimacy of originality easily by using standard method.

3.2 Ensuring validity of digital signature while keeping it for a long term

The digital signature used in electronic certifications essentially has a possibility that it may become unable to guarantee its validity as time advances, for instance, in such a case of expiration of a validity period or revocation of a public key certification, or keys and algorithms put under threat. Therefore, some schemes to recover such temporary restrictions are needed.

To deal with this situation, a technique for extending information concerning revocation of digital certifications and a secure time stamp to a digital signature, based on formats whose standardization are now underway in IETF (Internet Engineering Task Force) and ETSI (European Telecommunication Standards Institute), is developed (Fig. 2). The technological development is implemented as a member of long-term reservation technique for computerized documents examining consortium as a part of "E-Government information security infrastructure technical development project –

validity date extension technical development of electronic signature for preservation of documents for a long term" by IPA.

It is assumed that in comparison with the formats whose standardization are being underway, extension and preservation of signatures are performed by the interested party itself such as a creator of a digital signature or a verifier. The technique now developed is improved in that extension and preservation procedure of signature can be entrusted to third parties.

By using the technique, it is made possible to provide validity period extension service of digital signature for recovering temporal restriction held by digital signatures as a service by a third party alone.

3.3 Guarantee of created date and time of the electronic documents

The digital signature can guarantees the creator of data or that the data has not been altered, however, cannot guarantee time, for example, what date and time the data is created.

A secure time stamp is a technique that guarantees the following two items for digital data: 1. The digital data existed at a particular point in time; 2. The digital data has not been altered at or after the particular point in time. The time stamp is a format made in a manner in which a digital signature is appended to a combination of a hash value of data that a Time Stamp authority desires to prove, and time information (Fig. 3), whose standardization effort has been underway in IETF, and is standardized as RFC3161.

We develop time stamp server software in conformity with IETF standard, and utilize it for creating electronic certifications and extension of validity periods of digital signatures.

Features of secure storage are as a whole shown below.

1. Guarantee authenticity of electronic documents by issuing an electronic certification whereto a secure time stamp is appended.
2. Maintain the validity of the digital signature by means of validity period extension of signature, and guarantee authenticity of signed documents and electronic certifications for long periods of time.
3. Agents as third parties entrusted by the signer or the verifier can preserve the electronic signed documents for long periods of time.
4. Standard data formats are adopted, therefore, verification of authenticity needs not be entrusted to an authority but can be implemented by the client itself (the signer, the verifier, the arbitrator).

4. Application of the secure storage for the electronic medical chart

It was suggested in the report on "Commission on practical use of medical records such as medical charts" of Ministry of Health and Welfare held in June 1998

that computerization of medical records should be further promoted. Further, the criterion for preservation by electronic media is specified in "On storage of electronic media such as medical records" released on April 22, 1999. The criterion depends on "authenticity, legibility and storage stability (Three principles of electronic storage)" as a basis, and further refers to "privacy protection" and "evidential capacity, probative value".

It is hereinafter described positioning, necessity and case examples of application of the secure storage for the electronic medical chart.

4.1 Mutually complementally relation between technical measures and operational measures

When the electronic medical chart is introduced, technical measures and operational measures are to address securement of authenticity, legibility, storage stability, privacy protection and evidential capacity, probative value, in a mutually complementary manner. Therefore, the more reliable technical measures become, the simpler operable measures become. It is desirable for personnel in charge of promoting introduction of electronic medical chart system to introduce a system with adequate technical measures performed and with operational cost kept low. The secure storage is able to support securement of three principles of electronic storage from the technical aspect, and makes it easy to ensure evidential capacity and probative value.

4.2 Ensuring evidential capacity and probative value

According to "Report of system reexamination working group of Headquarters for promotion of advanced information and communications society as of June 1996", it is stated that "for ensuring evidential capacity and probative value of electronic data, it is necessary to improve the reliability of electronic data by ensuring integrity of input and output of data, as well as by diminishing possibility of data alteration, and further to clarify one who owes the responsibility for the reliability of electronic data". Probative value depends on the arbitrary judgment by judges. On the other hand, the evaluation depends on the evaluation of integrity of electronic data etc., therefore, it is extremely important feature that integrity of electronic data is guaranteed by technical measures.

The secure storage has "electronic notary function" to ensure authenticity of electronic documents by issuing electronic certifications that indicate "user", "contents of data", "time", and "type of commitment or operation (such as whether input or output is performed)" according to details of data input and output by users. Due to the function, the secure storage can technically guarantee the integrity and be of help to ensure evidential capacity and probative value.

4.3 Diminishing possibility of data alteration

There exists an obligation to preserve medical charts for five years according to medical practitioners law. Electronic medical charts only need smaller storage space in comparison to the conventional paper-based medical charts, therefore, electronic

medical charts can be stored longer periods of time. Some advanced clinics are promoting a project to store lifetime amount of electronic medical charts of patients under the concept of "Lifelong use of electronic medical charts". In such a case when long-term storage for nearly 100 years is needed, ciphers commonly used at the present time will become obsolete, and it will become difficult to prevent alteration of data only by appending regular electronic signatures. Therefore, the secure storage adopts a system that sustains long-term storage using the validity period of signature extending technique.

4.4 Cooperation with the electronic medical chart system

The secure storage is only a storage and it stores medical charts in their state securely for long periods of time, therefore, the medical charts are needed to be stored in such a structure that the medical charts will be legible into the future to guarantee legibility of data stored for long periods of time. However, the electronic medical chart systems are developed by vendors of healthcare information systems in their own specifications, and therefore, when electronic medical charts are stored in data structures unique to each vendor, it may become impossible to indicate medical charts when systems are replaced or so, and it may become impossible to guarantee long-term legibility.

Therefore, we have established a scheme which guarantees cooperation with electronic medical chart system into the future and which guarantees legibility of medical charts on their own by storing as medical charts XML files in "The Japanese set of identifiers for medical record information exchange" (hereinafter referred to as "J-MIX") drafted by projects sponsored by Ministry of Health and Welfare in fiscal year 1999. The electronic medical chart system has only to transfer medical chart data as a XML file in J-MIX format to the secure storage on the day the data is settled and processed. The rest of the securement process of the three principles of electronic storage is implemented by electronic certifications managed by the secure storage, therefore, there is no need to establish a high cost electronic storage system at the electronic medical chart system side.

4.5 Case example of application to electronic medical chart system

The system described in the figure on the page of summary is adopted in the healthcare information network promotion project in Minami-Bousou area whose center is Kameda Medical Center of Tetsusyou-kai Healthcare Corporation in "Healthcare-centered network promoting project by utilizing advanced IT – Regional healthcare informatization with a focus on medical records" by Ministry of Economy, Trade and Industry. In this project, to realize the three principles for electronic storage in the electronic medical chart system for regional alliances, a backup of the original of the medical charts in an ASP-type electronic medical chart system for regional alliances is stored as a XML file in J-MIX format.

5. Conclusion

In computerization of documents, "long-term storage of original" regarded as a final step of the lifecycle of documents has been left behind, and has been a strong factor which prevents moving from a paper-based system. The secure storage is a technique that enables storing electronic original for long periods of time by making full use of the digital signature technique which has achieved legal support by implementation of Electronic Signature Law.

In the medical field, external preservation of electronic medical charts has been considered in Ministry of Health, Labour and Welfare, and it is assumed that the ASP-type electronic medical chart system which has been conventionally impossible will be widely used in future. Further, there is a need to store the electronic medical charts conventionally stored inside hospitals in a further robust data center. By utilizing the secure storage as what fulfills such needs, the electronic medical chart system can be established in low cost.

The secure storage has an electronic notary function to guarantee various commitments to electronic documents, and can be utilized not only for storage of electronic original but also for nonrepudiation in a case of exchanging electronic data or electronic documents such as EDI. We think it is possible for the secure storage we propose to contribute to promoting paperless and introducing information technology in medical and many other fields.

Secure Storage セキュアストレージ —電子カルテへの適用—

宮崎一哉*
若原秀幸**

Denshi Carte e no Tekiyo

要旨

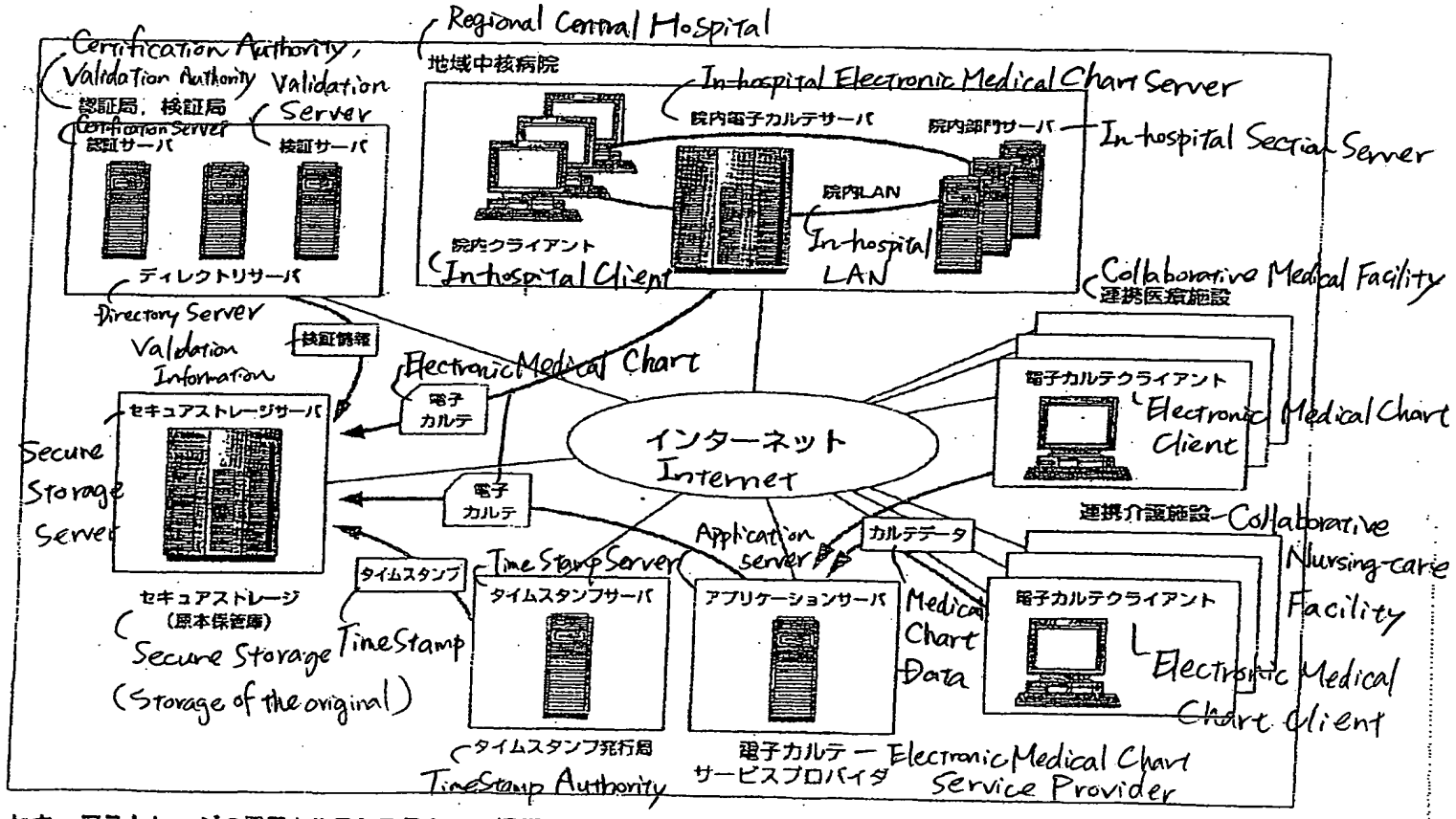
企業や官公庁などにおける業務の電子化に伴い，重要な文書の電子化が急速に進行している。近い将来，電子化される文書の中には，数十年といった長期間にわたって保存することが義務付けられるものも含まれることが見込まれる。

一般に，紙に書かれた文書やマイクロフィルムに記録された文書と異なり，電子化されたデータには改ざん(竄)，漏えいなどの脅威が付きまとうが，こうした脅威に対抗し，原本性を保証することによって電子文書を法的に有効な実効ある文書と位置付けることができ，その結果，真のペーパーレス化が推し進められることになるものと考える。

セキュアストレージは，デジタル署名などのPKI(Public Key Infrastructures：公開かぎ(鍵)基盤)に立脚した情報セキュリティー技術を利用したものであり，電子文書の原本性を長期間にわたって保証する技術である。標準的なフレームワークを用いており原本性の検証が容易であること，デジタル署名の有効性延長技術を備えており原本性を長期間保持できることなどが特長である。

医療分野でも電子化が推進されており，カルテの電子保存に関する指針も示されている。今回，医療現場に普及しつつある電子カルテシステムに対しセキュアストレージを適用し，その有効性を検討した。

今後，セキュアストレージが，医療分野にとどまらず，多くの分野におけるIT化やペーパーレス化に資するものと考える。



セキュアストレージの電子カルテシステムへの適用

地域中核病院の院内クライアント，連携医療施設，連携介護施設の電子カルテクライアントで生成されたカルテデータは，それぞれ，院内電子カルテサーバ及び電子カルテサービスプロバイダを経由して電子カルテの原本がセキュアストレージで保管される。セキュアストレージでは，電子カルテの真正性を保証するために電子証書を発行管理し，また，真正性を長期間保証するために安全なタイムスタンプや認証書の検証情報を収集し，デジタル署名の拡張を行う。

*情報技術総合研究所　**医療システム統括部

1. まえがき

企業や官公庁などにおける業務の電子化に伴い，契約関係書類，行政文書，電子カルテなど，重要な文書の電子化が急速に進行している。近い将来，電子化される文書の中には，5年，10年，30年，それ以上の長期間にわたって保存することが義務付けられるものも含まれることも想像に難くない。

一般に，紙に書かれた文書やマイクロフィルムに記録された文書と異なり，電子化されたデータには，改竄やすり替え等が容易で痕跡も残らない，盗難，漏えい，盗み見が大量かつ秘密裏に行われやすい，などの安全面での脅威がつきまとう。こうした脅威に対抗し，原本性を保証[1]することによって電子文書を法的に有効な実効ある文書と位置付けることができ，その結果，真のペーパーレス化が推し進められることになるものと考える。原本性を保証するための効果的な技術として，デジタル署名がある。2001年4月1日に電子署名法(電子署名及び認証業務に関する法律)が施行されたことにより，その効果が法的に裏付けられることとなった。ところが，デジタル署名はその効果とともに幾つかの問題点を併せ持つため，単にデジタル署名を電子文書に付与するだけでは長期間原本性を保証することはできない。

今回開発したセキュアストレージ技術は，デジタル署名などのPKIに立脚した情報セキュリティ技術を利用した技術であり，これによって電子文書の原本性を長期間にわたって保証することができる。

本稿では，セキュアストレージの概要と，一例として電子カルテシステムへの適用について述べる。

2. 電子文書長期保存の必要性

各種契約書，行政文書，電子カルテなど，法的又は商習慣的に原本を長期間保存することが要請されている文書が存在する。電子化が進む中，前章で述べた電子文書のぜい(脆)弱性が原因で，この要請にこたえるためには余儀なく紙媒体やマイクロフィッシュで長期保存をしていたのが実情である。

電子文書の原本性を確保するためには，電子文書が，いつ，だれによって作成されたもの(又は承認されたもの)であり，それが改竄されていないこと(これらをまとめて電子文書の真正性と呼ぶこととする。)を保証する仕組みが必要となる。PKIにおけるデジタル署名は，電子文書の真正性確保のための最も有力な方法と目されており，昨年施行された電子署名法によって法的な裏付けも得られた。

ところが，単純にデジタル署名を用いただけでは，"だれが作成したものでありそれが改竄されていない"ことまでは保証し得るが，"いつ"を保証することができない。また，デジタル署名の有効性には，時間的な制約が存在する。つまり，公開鍵証明書(認証書)の有効期限切れや失効，デジタル署名に用いられる鍵やアルゴリズムの危たい(殆)化などにより，デジタル署名の有効性は失われてしまう。そこで，デジタル署名を利用して長期間にわたって電子文書の真正性を確保するには，何らかの新しい工夫が必要となる。

3. セキュアストレージ

セキュアストレージは，長期間にわたって真正性を確保しながら電子文書を保存するための技術である。その概要は次のとおりである。

3.1 電子証書による電子文書の真正性保証

セキュアストレージでは，クライアントからの要求により，文書の登録，検索，参照，削除などを実行する。このとき，以下の内容を保証するための電子証書を発行し，管理する(図1)。

- 文書の作成者又は登録依頼者
- 預かった文書が改竄されていないこと
- 文書に対する登録，検索，参照，削除などのアクセスの事実及び日時

電子証書は，対象文書のハッシュ，アクセス情報，そして3.3節で述べる安全なタイムスタンプ[2]などを含んだ情報とそれに対するデジタル署名で構成される。また，3.2節で述べるデジタル署名の有効性の長期にわたる保持技術により，長期間にわたり電子証書の有効性を保つことができる。従来から提案されている耐タンパーなハードウェアで原本性を確保する技術ではその正当性を客観的に検証することが極めて困難であったが，今回開発した技術は，PKIに基づくソフトウェアによって実現した技術であるため，第三者が標準的な手段で容易に正当性を検証することが可能である。

3.2 長期保存におけるデジタル署名の有効性の確保

電子証書で利用するデジタル署名は，公開鍵証明書の有効期限，失効，鍵やアルゴリズムの危殆化など，本来，時

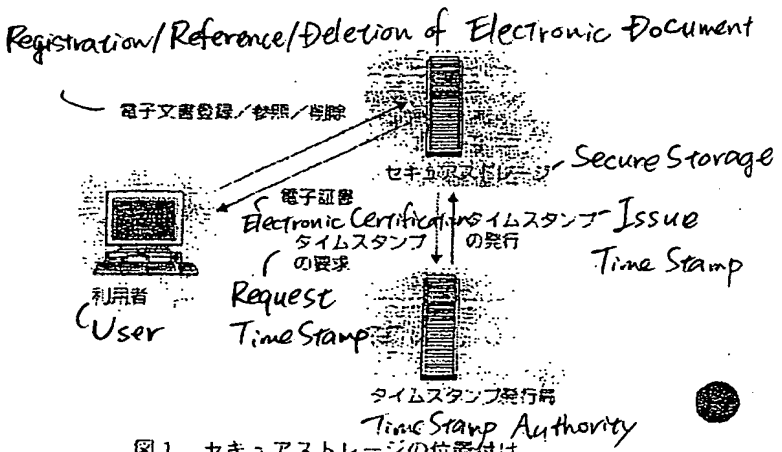


図1. セキュアストレージの位置付け
Fig.1 Positioning of Secure Storage

間経過に伴って有効性を保証できなくなる可能性をはらんでおり，このような時間的制約を乗り越えるための仕組みが必要となる。

この対応として，IETF(Internet Engineering Task Force)やETSI(European Telecommunications Standards Institute)で標準化が進められている書式[3][4]をベースとして，デジタル証明書の失効に関する情報や安全なタイムスタンプを時間経過とともにデジタル署名に対して拡張していく技術を開発した(図2)。この技術開発は，IPA事業「電子政府情報セキュリティ基盤技術開発事業 ― 長期保存文書のための電子署名期限延長技術開発 ― 」の一環として電子文書長期保存技術検討コンソーシアムの一員として実施したものである。

標準化の進められている書式はデジタル署名の作成者又は検証者といった当事者自らが署名を拡張し保管することが想定されていたが，今回の技術では署名の拡張及び保管処理を第三者に委託することができるよう改良を加えた。

この技術を用いることにより，デジタル署名の持つ時間的制約を克服するデジタル署名の有効性延長サービスを，第三者による単体のサービスとしても提供することが可能となる。

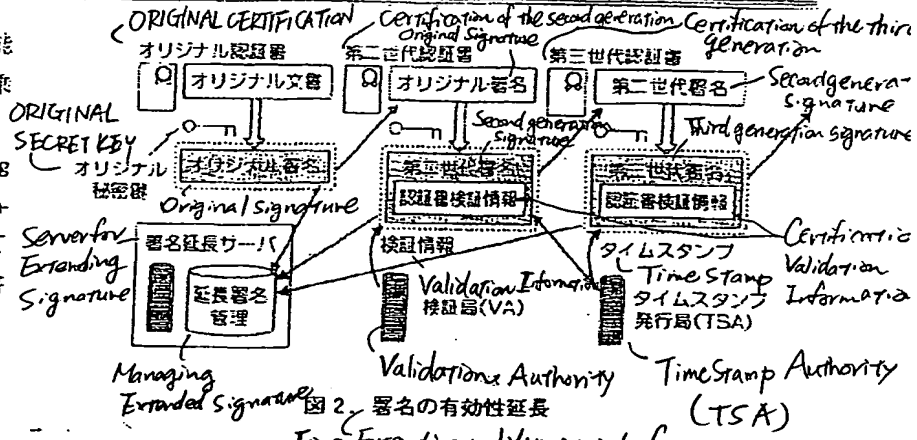


図2 署名の有効性延長

Fig.2 Extending validity period of signature

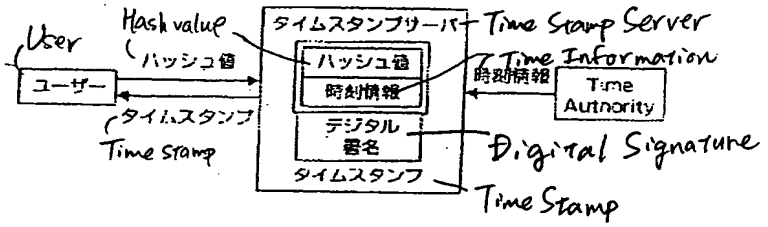


図3. 安全なタイムスタンプ

Fig.3 Secure timestamp

3.3 電子文書の作成日時の保証

デジタル署名は，データの作成者やデータが改竄されていないことを保証できるが，時刻に関する保証，例えばデータが作成された日時の保証はできない。

安全なタイムスタンプは，デジタルデータに対して，①ある時刻に存在していたこと，②その時刻以降に改竄されていないこと，の二つを保証する技術である。タイムスタンプは，TTP(Trusted Third Party：信頼できる第三者機関)であるタイムスタンプ発行局が証明したいデータのハッシュ値と時刻情報を組み合わせたものにデジタル署名を施した形式であり(図3)，IETFで標準化活動が進められており，RFC3161[5]として標準化された。

我々はIETF標準に準拠したタイムスタンプサーバソフトウェアを開発し，電子証書の作成やデジタル署名の有効性延長に利用している。

以下に，セキュアストレージの特長をまとめて示す。

(1) 安全なタイムスタンプ付きの電子証書を発行することにより，電子文書に対する真正性を保証

(2) 署名延長を用いてデジタルの署名の有効性を維持し，署名文書及び電子証書の長期にわたる真正性保証を実施

(3) 署名者又は検証者の委託を受け，第三者であるエージェントが電子署名文書の長期保存を実施可能

(4) 標準的データ形式を採用しており，真正性の検証をオーソリティに委託する必要がなく，クライアント(署名者，検証者，仲裁者)自身で実施することが可能

4. 電子カルテにおけるセキュアストレージの適用

平成10年6月，厚生省の"カルテ等の診療情報の活用に関する検討会"において診療情報の電子化を今後一層推進すべきとの報告がなされ，平成11年4月22日付の"診療録等の電子媒体による保存について"によって電子媒体による保存の基準が明確化された[6]。その基準は"データの真正性，見読性及び保存性"(電子保存三原則)を基本とし，"プライバシー保護"や"証拠能力・証明力"にまで言及するものとなっている。

以下，電子カルテにおけるセキュアストレージの位置付け，必要性，及び適用事例について述べる。

4.1 技術的対策と運用的対策による相互補完

電子カルテを採用する場合，真正性，見読性，保存性，プライバシー保護及び証拠能力・証明力の確保を，技術的対策と運用的対策の相互補完で対応することとなる。そのため，技術的対策が確実であればあるほど運用的対策が容易になる。電子カルテシステム導入推進担当者からすれば，運用コストを抑え十分な技術的対策を施したシステムの導入が望まれる。セキュアストレージは，電子保存三原則の確保を技術的側面からサポートし，証拠能力・証明力の確保を容易にすることが可能である。

4.2 証拠能力・証明力の確保

「高度情報通信社会推進本部制度見直し作業部会報告書 平成8年6月」によれば，"電子データの証拠能力及び証明力の確保については，データの入力及び出力の正確性を確保するとともに，データの改変の可能性を減殺することにより電子データの信頼性を高め，かつこれに対する責任

の所在を明らかにする必要がある"としている。証明力については裁判官の自由な判断にゆだねられているが，その評価は電子データの正確性等の評価に依存するため，技術的対策によって正確性が保証されることは非常に重要である。

セキュアストレージは，利用者のデータ入力及び出力内容に応じ，"利用者""データの内容""その時刻""コミットメント又は操作の種類(入力したか出力したかなど)"を示す電子証書を発行することにより，電子文書の真正性を確保する"電子公証機能"を持っている。これにより，技術的にその正確性を保証することができ，証拠能力・証明力の確保に資することができる。

4.3 データの改変の可能性の減殺

カルテは医師法によって5年間の保存義務があるが，電子カルテは，従来の紙カルテに比べ保管スペースが小さくて済むようになることから，より長期の保存が可能となる。先進的な病院では，"生涯電子カルテ"のコンセプトの下に，患者の一生分の電子カルテを蓄積する計画を推進している。このような100年近い長期保存を行う場合，現在一般的に利用されている暗号が陳腐化し，通常の電子署名を行っただけでは改竄防止が困難になる。そのため，セキュアストレージでは，署名延長技術を用いて長期保存にも耐えるシステムを採用している。

4.4 電子カルテシステムとの連動

セキュアストレージはあくまで保管庫であり，カルテをそのままの状態で安全に長期保存するものであるため，長期保存したデータの見読性を保証するには保存するカルテが将来にわたって容易に見読可能な構造でなければならない。しかし，電子カルテシステムは医療情報システムベンダー各社が独自の仕様で開発を行っており，各社独自のデータ構造のまま保存した場合，システムのリプレース等によってカルテの表示が不可能になる可能性も否定できないため，長期的な見読性の保証ができなくなる。

そこで，平成11年度厚生省委託事業によって作成された「電子保存された診療情報録の交換のためのデータ項目セット」(以下"J-MIX"という。)のXMLファイルをカルテとして保存することにより，将来にわたって電子カルテシステムとの連携を保証するとともに，カルテ単独での見読性を保証する仕組みを構築した。電子カルテシステムは当日確定処理されたカルテデータをJ-MIX形式のXMLファイルとしてセキュアストレージに転送するだけでよく，それ以降の電子保存三原則の確保についてはセキュアストレージが管理する電子証書によって行うため，電子カルテシステム側では高コストの電子保存システムを構築する必要がない。

4.5 電子カルテシステムへの適用事例

要旨のページの図のシステムは，経済産業省の「先進的IT活用による医療を中心としたネットワーク化推進事業 ― 電子カルテを中心とした地域医療情報化 ―」において，医療法人鉄蕉会による亀田病院を中心とした南房総地域の医療情報ネットワーク推進事業に採用された。この事業では，地域連携のための電子カルテシステムの電子保存三原則対応を実現するために，地域連携用のASP型電子カルテシステムのカルテ原本のバックアップをJ-MIX形式のXMLファイルとして保管している。

5. むすび

文書の電子化において，文書のライフサイクルの最終ステップに位置付けられる"原本の長期保管"が取り残されており，これがペーパーレス化を阻害する大きな要因となってきた。セキュアストレージは，電子署名法の施行によって法的裏付けを得たデジタル署名技術を駆使して，電子的な原本を長期間にわたって保存することを可能とする技術である。

医療分野では，厚生労働省において電子カルテの外部保存についての検討が行われており，従来は不可能であったASP型の電子カルテシステムが今後普及していくことが予想されている。また，従来病院内で保管していた電子カルテを，より堅牢なデータセンターに保管したいという要望もある。これらの受け皿としてセキュアストレージを活用することで低コストでの電子カルテシステム構築が可能となる。

セキュアストレージでは，電子文書に対する様々なコミットメントを保証する電子公証機能を保有しており，電子原本の保管のみでなく，EDIのような電子データや電子文書の交換における否認防止にも活用できる。我々の提案するセキュアストレージは，医療を始めとする他の多くの業界におけるペーパーレス化，IT化の推進に貢献することができると考える。

参考文献

(1) 総務庁共通課題研究会報告書：インターネットによる行政手続の実現のために(2000-3)

(2) 宮崎一哉：電子文書における署名とタイムスタンプについて，三菱電機技報，75，No.2，152～154 (2001)

(3) RFC3126：Electronic Signature Formats for long term electronic signatures (2001-9)

(4) ETSI Standard：ETSI TS 201 733 Electronic Signature Formats (2000-12)

(5) RFC3161：Time-Stamp Protocol(TSP) (2001-8)

(6) 財団法人医療情報システム開発センター：診療録等の電子媒体による保存に関する解説書 (1999-10)

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☑ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☑ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.